

What is claimed is:

1. A Virtual Private Network (VPN) communication method employed for a security gateway apparatus connecting between a local area network (LAN) and a wide area network (WAN) including a public network, the communication method comprising the steps of:
 - a) adding a Dynamic Host Configuration Protocol (DHCP) communication option to an Internet Key Exchange (IKE) data, when establishing an IKE communication with a terminal outside the LAN having a dialup connection with the WAN;
 - 10 b) distributing an IP address to the terminal outside the LAN during the IKE communication; and
 - c) establishing a Security Architecture for the Internet Protocol (IPsec) communication that follows the IKE communication, wherein the gateway apparatus designates an IP address for the outside terminal from a tunneled IP packet.
- 20 2. The VPN communication method employed for the security gateway apparatus as defined in claim 1, wherein an IP address and a subnet mask address, which have same segments as those of the LAN, are distributed to the outside terminal, thereby the outside terminal can be virtually regarded as a terminal on the LAN.
- 25 3. The VPN communication method for the security gateway apparatus as defined in claim 1, wherein the outside terminal is provided, during the IKE communication, with a private IP address that is used on the LAN, in a case that the LAN is configured with private IP addresses, whereby the outside terminal is allowed to access to a terminal on the LAN.

Sub A 17

4. The VPN communication method for the security gateway apparatus according to any one of claims 1 through 3, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the
5 IKE communication.

5. The VPN communication method for the security gateway apparatus according to any one of claims 1 through 3, wherein the DHCP communication option contains an IP address and a subnet mask.

10

6. A security gateway apparatus connecting between a local area network (LAN) and a wide area network (WAN) including a public network, the apparatus comprising:

15 a) a Dynamic Host Configuration Protocol (DHCP) option adding

section adding a DHCP communication option to an IKE data when establishing an IKE communication with a terminal outside the LAN having a dialup connection with the WAN;

b) an IP address distribution section distributing an IP address to the outside terminal during the IKE communication; and

20 c) an IPsec communication section performing an IPsec communication that follows the IKE communication,

wherein, the gateway apparatus designates an IP address for the outside terminal from a tunneled IP packet.

25

7. The security gateway apparatus as defined in claim 6, wherein an IP address and a subnet mask address, which have same segments as those of the LAN, are distributed to the outside terminal, thereby the outside terminal can

be virtually regarded as a terminal on the LAN.

8. The security gateway apparatus as defined in claim 6, wherein the outside terminal is provided, during the IKE communication, with a private IP address which is the same as one used on the LAN in a case that the LAN is configured with private IP addresses, whereby the outside terminal is allowed to access to a terminal on the LAN.

Sub A2

9. The security gateway apparatus according to any one of claims 6 through 8, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

10. The security gateway apparatus according to any one of claims 6 through 8, wherein the DHCP communication option contains an IP address and a subnet mask.

add A3